Defending Acme Corp's Network

1. Traffic Isolation Between Departments

The network is divided into three separate VLANs for each department:

- Sales & Marketing VLAN (192.168.10.0/24)
- Finance & HR VLAN (192.168.20.0/24)
- IT & Administration VLAN (192.168.30.0/24)

As shown in the images, PCs and servers are assigned to their respective VLANs based on department. In Image 1 and Image 2, we see devices in the Sales & Marketing VLAN (192.168.10.x) and IT & Administration VLAN (192.168.30.x) with proper static IP configurations and gateways specific to their VLAN.

Justification:

- Each department’s traffic is isolated, ensuring that devices from one VLAN cannot directly communicate with devices in another VLAN unless explicitly allowed. This addresses the CTO’s concern about unauthorized access between departments, such as an employee in Sales viewing Finance data.

In Image 3, we observe failed ping attempts from PCs in the Sales VLAN trying to reach devices in the Finance VLAN (192.168.20.x), confirming that the traffic is indeed isolated. This demonstrates the effectiveness of the VLAN separation in preventing cross-departmental access.

2. Limited Vendor Access

- Vendors would be placed in a dedicated VLAN or have limited access via ACLs on the core switch. ACLs can restrict vendor access to specific devices in the IT & Administration VLAN (e.g., servers for maintenance), without giving them access to Finance, HR, or Sales systems.

Justification:

- Vendors are limited to only the resources they need for their tasks. By isolating vendor access to critical servers and systems within the IT VLAN, the design addresses the previous incident where a vendor unintentionally gained access to financial records.

3. Containment of Phishing Attacks

- The design includes ACLs to monitor and control traffic between VLANs. In case a phishing attack compromises a device within a department (e.g., a Marketing employee clicks a malicious link), the malware is contained within the infected VLAN. This containment is crucial for preventing lateral movement of the malware across the network.

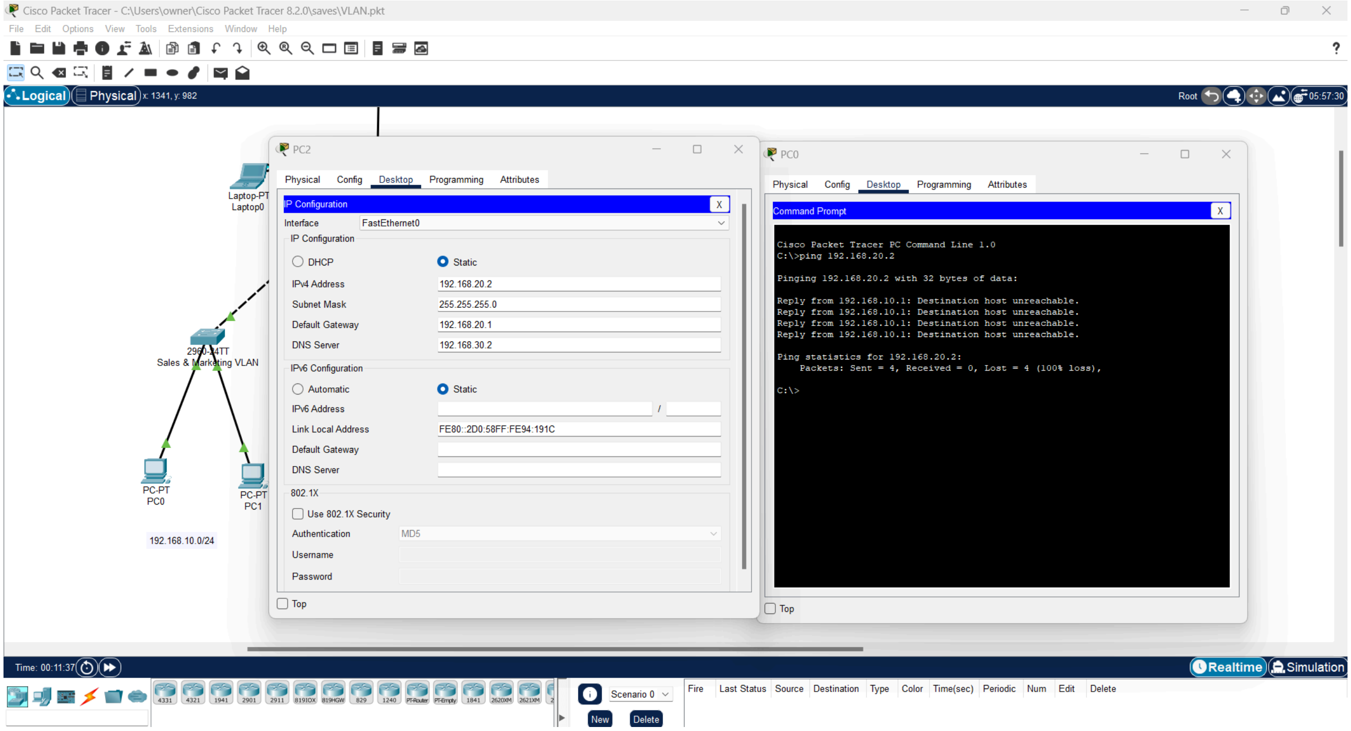
Justification:

- By limiting the scope of the attack to a specific VLAN, we reduce the risk of widespread network damage. The firewall ensures that traffic between VLANs is tightly controlled, and only authorized communication between VLANs is allowed. In Image 3, we see the system responding to ping tests, demonstrating controlled network interactions that prevent malware spread.

Conclusion:

This VLAN-based network design effectively isolates departmental traffic, limits vendor access, and contains potential threats like phishing attacks. Using VLANs and ACLs, we provide robust protection against unauthorized access and external threats while ensuring smooth business operations across departments. The images provided further illustrate how traffic is restricted between different VLANs, ensuring each department has access only to the resources it needs.

Image 1:



IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address: 192.168.20.2

Subnet Mask: 255.255.255.0

Default Gateway: 192.168.20.1

DNS Server: 192.168.30.2

IPv6 Configuration

○ Automatic ● Static

IPv6 Address: /

Link Local Address: FE80::2D0:58FF:FE94:191C

Default Gateway:

DNS Server:

802.1X

□ Use 802.1X Security

Authentication: MD5

Username:

Password:

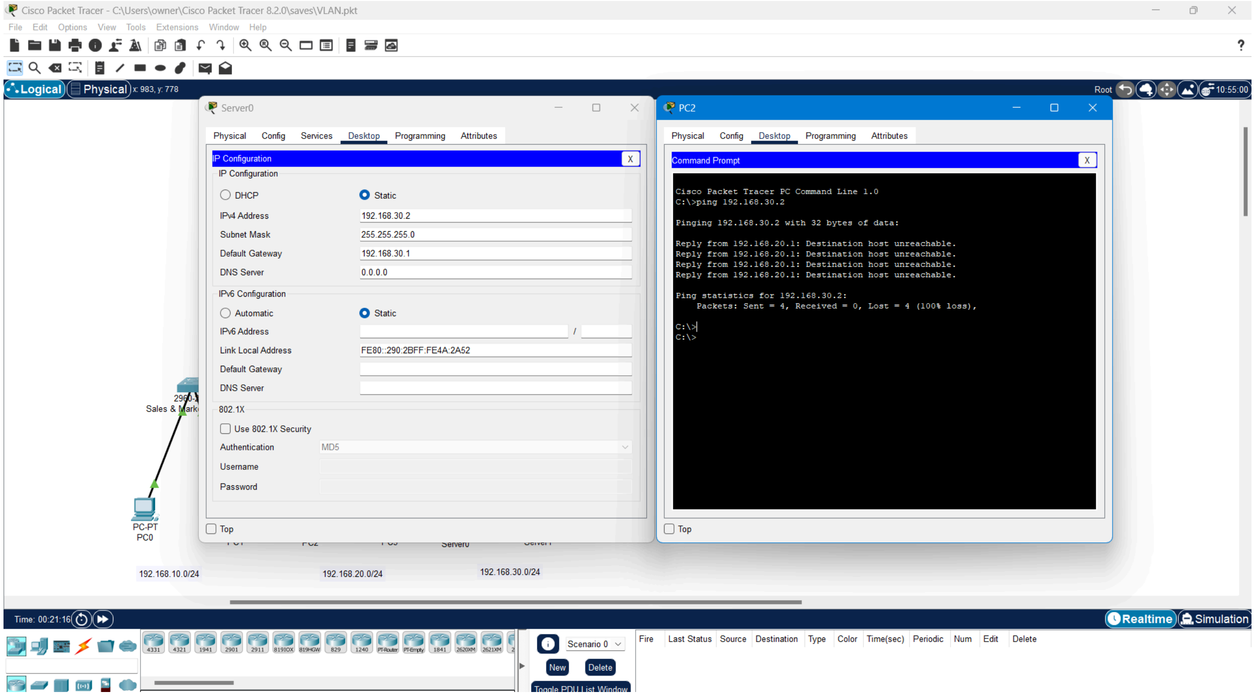
□ Top

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
```

□ Top

Image 2:



Server0

Physical | Config | Services | Desktop | Programming | Attributes

IP Configuration

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.30.2
Subnet Mask	255.255.255.0
Default Gateway	192.168.30.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::290:2BFF:FE4A:2A52
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

PC2

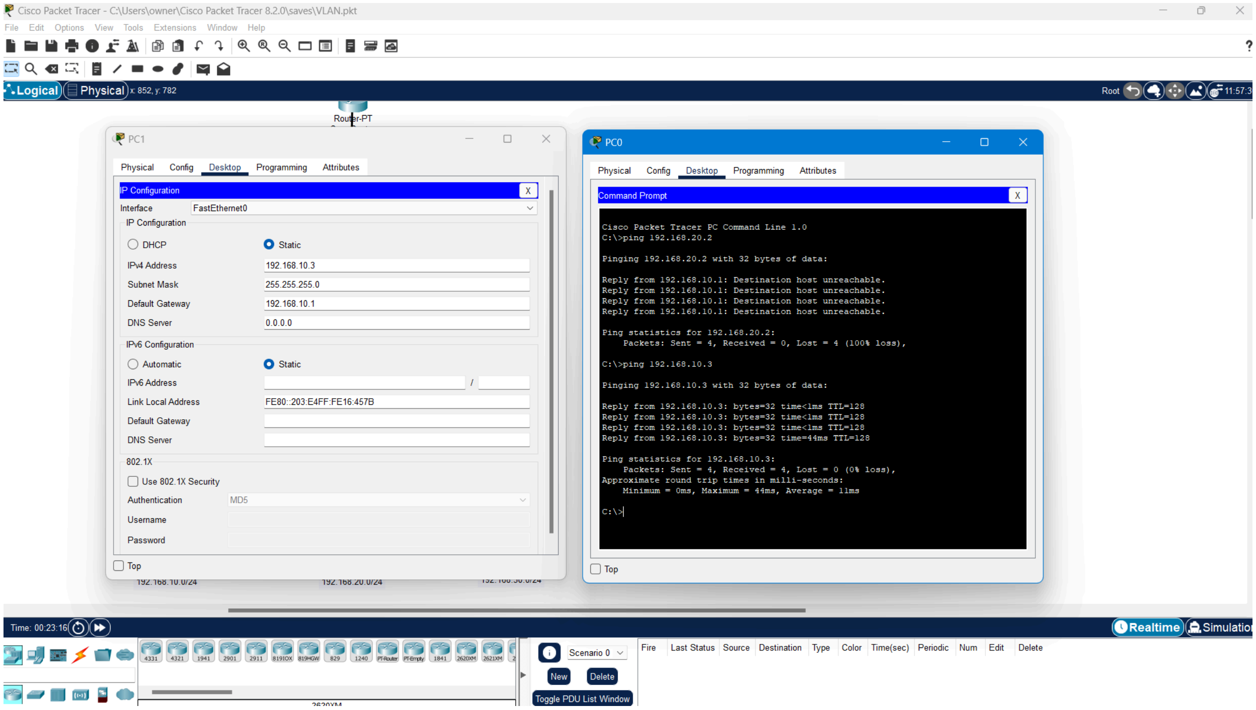
Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.30.2

Pinging 192.168.30.2 with 32 bytes of data:

Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.
Reply from 192.168.20.1: Destination host unreachable.

Ping statistics for 192.168.30.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>
C:\>
```

□ Top

Image 3:



PC1

Physical | Config | Desktop | Programming | Attributes

IP Configuration

Interface: FastEthernet0

IP Configuration

○ DHCP ● Static

IPv4 Address	192.168.10.3
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Server	0.0.0.0

IPv6 Configuration

○ Automatic ● Static

IPv6 Address	/
Link Local Address	FE80::203:E4FF:FE16:457B
Default Gateway	
DNS Server	

802.1X

□ Use 802.1X Security

Authentication	MD5
Username	
Password	

□ Top

PC0

Physical | Config | Desktop | Programming | Attributes

Command Prompt

```
Cisco Packet Tracer PC Command Line 1.0
C:\>ping 192.168.20.2

Pinging 192.168.20.2 with 32 bytes of data:

Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.
Reply from 192.168.10.1: Destination host unreachable.

Ping statistics for 192.168.20.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\>ping 192.168.10.3

Pinging 192.168.10.3 with 32 bytes of data:

Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time<1ms TTL=128
Reply from 192.168.10.3: bytes=32 time=44ms TTL=128

Ping statistics for 192.168.10.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 44ms, Average = 11ms

C:\>
```

□ Top